

### **REMARKS**

This amendment is in response to the Official Action dated July 27, 2007. Claims 11 and 17 have been amended to include the subject matter of former claim 13, claims 1, 2, 7, 13, 15, 16 and 18 have been cancelled, and claims 19-32 have been added; as such, claims 3-6, 8-12, 14, 17, and 19-32 are currently pending in connection with the present application. Claims 3, 9-11, 17, 19, 20, and 28 are independent claims. Reconsideration and allowance is requested in consideration of the claim amendment and the following remarks.

#### **35 U.S.C. § 112 Rejections**

Claims 10 and 18 have been rejected under 35 U.S.C. § 112.

Claim 10 has been amended to recite a tangible recordable medium, in line with the Examiner's suggestions. Claim 18 has been cancelled.

Accordingly, withdrawal of the rejection is respectfully requested.

#### **35 U.S.C. § 101 Rejections**

Claims 10 and 18 have been rejected under 35 U.S.C. § 101 based upon the allegation that the claims are directed to non-statutory subject matter, particularly a software application.

Claim 10 has been amended to recite a tangible recordable medium, in line with the Examiner's suggestions. Claim 18 has been cancelled.

Accordingly, withdrawal of the rejection is respectfully requested.

#### **35 U.S.C. § 103 Rejections**

Claims 1-18 have been rejected under 35 U.S.C. § 103(a) as being obvious in view of Pare, Jr. et al. (U.S. Patent No. 6,662,166, hereinafter "**Pare**"). Applicant respectfully traverses this rejection.

Claim 11 has been amended to include the subject matter of former dependent claim 13. Former claim 13 has been cancelled. Thus, former claim 13 is now claim 11. Claim 17 has also been amended to is the subject matter of former claim 13.

Claims 1, 2, 7, 13, 15, 16 and 18 have been cancelled.

Pare discloses a system for authorizing automatic payments using biometric samples (*see* abstract). Fig. 1 illustrates a Party Identification Apparatus (PIA) 1 with a biometric sensor 2, such as a fingerprint or iris scanner. The PIA allows consumers to transact purchases without institutionally issued IDs, such as credit cards. The PIA transmits biometric information obtained by biometric sensor 2 to a data processing center 4 (in Fig. 2) which acts as a key to retrieve credit/debit account information. Pare depends on the consistency of the biometric data. The system relies on a consistent, reproducible, biometric sample to ensure reliable access to the user's transactional information. That is, *the biometric (authentication) information must remain consistently reproducible by different PIAs using different biometric samples* (Pare at c. 5, ll. 7-9). Thereafter, the user can make purchases without "presenting any personalized man-made tokens (Pare at c. 5: ll. 22-25).

### **Claim 3**

Claim 3 recites:

*An information management apparatus for generating an image to be displayed on a predetermined information processing terminal, the information management apparatus comprising:*

*generating means for generating a first authentication image to be used to*

*authenticate a user based on a predetermined original image,*

*providing means for providing the information processing terminal with the first*

*authentication image generated by the generating means,*

*authenticating means for authenticating the first authentication image which is provided by the information processing terminal through a control device that controls the reading of an image displayed on the information processing terminal, and*

*display control means for displaying a second authentication image instead of the first authentication image displayed on the information processing terminal when the authenticating means verifies that the first authentication image is authentic.*

***“generating means for generating a first authentication image ... providing means for providing the information processing terminal with the first authentication image, [and]... authenticating means for authenticating the first authentication image which is provided by the information processing terminal...”***

Claim 3 recites two devices: an information management apparatus (IMA) and an information processing terminal (IPT).

The information management apparatus (IMA) has means for (i) generating a first authentication image based on a predetermined original image; (ii) providing the first authentication image to the information processing terminal (IPT); (iii) authenticating the first authentication image when the image is provided by the IPT through a control device; and (iv) displaying a second authentication image on the IPT after verifying that the first authentication image is authentic.

**Therefore, in order for the IMA to authenticate the first authentication image from the IPT, in step (iii), the IMA must first create the authentication image and provide the authenticated image to the IPT, in steps (i) and (ii). *It is impossible to authenticate an image from the IPT if the IPT does not receive the image first.***

Pare discloses a different process. **Pare discloses comparing two separate samples, obtained from separate scanners, at two separate time periods to identify if the two samples are the same, within a reasonable margin of error.** In Pare, a Party Identification Apparatus

(PIA) 1 obtains a biometric sample (e.g. a fingerprint or iris scan) using a biometric sensor 2. The PIA then transmits biometric information obtained by biometric sensor 2 to a data processing center 4 (in fig. 2) which compares the new biometric sample to another pre-existing biometric sample.

By contrast, claim 3 recites having an **Information Management Apparatus (IMA) verify the authenticity of an authentication image on an Information Processing Terminal (IPT), the authentication image having been originally provided to the IPT by the IMA.**

The distinctive operations Pare and claim 3 are drastically different. Pare requires that a user provide biometric samples that can be used to reproduce similar identifiable biometric patterns. By contrast, claim 3 does not require near reproduction using different samples, but instead transfers an image generated at an IMA to the IPT, so that the IPT can authenticate itself to the IMA at a later time. **Pare does not provide any motivation for a first device that creates and transfers an image to a second device, where the second device can then use the image to authenticate itself to the first device.**

Page 4 of the final office action compares the authentication image, in claim 3, to a biometric sample obtained from the physical person by the PIA using a biometric sensor. The office action explains that the biometric sample is then transmitted to a data processing center (DPC) to determine whether the biometric sample matches a previous biometric sample taken from the user.

The distinction between claim 3 and Pare is clearly evident. Pare discloses comparing two separate samples, obtained from separate scanners, at two separate time periods to identify if the two samples are the same, within a reasonable margin of error. Pare does not disclose the creation of an authentication image, which is then transmitted to an IPT, or comparable terminal device for use in later authentication.

- Accordingly, Pare does not teach or suggest, nor would Pare motivate one of ordinary skill to produce a “*generating means for generating a first authentication image ... providing means for providing the information processing terminal with the first authentication image,*

*[and]... authenticating means for authenticating the first authentication image which is provided by the information processing terminal...*” For similar reasons, claims 9 and 10 are also patentable over Pare.

***“generating means for generating a first authentication image...[and]... authenticating means for authenticating the first authentication image which is provided by the information processing terminal”***

In claim 3, the image generated by the IMA is provided to the IPT for use in authentication. Therefore, claim 3 generates an **authentication image that acts as a token** for accessing data, information, or funds.

Pare neither suggests nor renders obvious a *“generating means for generating a first authentication image... [and]... authenticating means for authenticating the first authentication image which is provided by the information processing terminal,”* because doing so would contradict the very purpose of the Pare invention, i.e., to provide **“Tokenless Biometric Electronic Debit and Credit Transactions”** without the need to possess any personalized tokens (Pare, title and c. 3, l. 66 – c. 4, l. 5). The creation of an authentication image based on a predetermined original image (i.e. an image known beforehand) is contrary to Pare, since such an image would require the use of a personalized, unique token.

- Accordingly, Pare does not teach or suggest, nor would Pare motivate one of ordinary skill to produce a *“generating means for generating a first authentication image...[and]... authenticating means for authenticating the first authentication image which is provided by the information processing terminal.”* For similar reasons, claims 9 and 10 are also patentable over Pare.

#### **Claim 4**

Claim 4 recites:

*An information management apparatus according to claim 3, wherein*

*the generating means generates further the second authentication image when the authentication means verifies that the first authentication image is authentic, and the display control means displays the second authentication image on the information processing terminal by providing the information processing terminal with the second authentication image generated by the generating means.*

***“the generating means generates further the second authentication image when the authentication means verifies that the first authentication image is authentic.”***

Claim 4 discloses that the same generating means, in the IMA, that generates the first authentication image also generates the second authentication image.

First, Pare does not teach the creation of a second authentication image, i.e., an image used for authentication. While Pare teaches that a first biometric sample is used to provide access to a user's accounts, this biometric sample is not produced by either the data processing center (DPC) (i.e., the only element of Pare comparable to an authentication device) or the original sample provided to the PIA device for later use in authentication.

Second, even if it were possible for the DPC to produce a second biometric sample associated with the given user, **Pare does not teach that the DPC produces a second authentication image/biometric sample using the same generation means used to provide the first sample.** Instead, Pare teaches reusing the original biometric sample perpetually for comparison to later transactions. Pare, does not change the biometric sample used to authenticate a user after a given transaction is verified.

Page 5 of the final office action argues that Pare's tokenless biometric electronic debt and credit transaction system is comparable to the claimed token-based transaction system. In particular,

the office action argues that it would be possible for Pare to produce multiple authentication images despite the fact that a person's biometric information is static and unique.

Contrary to the assertion in the office action, it is impossible for a single individual to produce *two unique and different biometric samples of the same type* which can be reliably used to identify that user. Accordingly it would be impossible for Pare to produce a second authentication image using the same means to authenticate a given user.

- Accordingly, Pare does not teach or suggest, nor would Pare motivate one of ordinary skill to that *“the generating means generates further the second authentication image when the authentication means verifies that the first authentication image is authentic.”*

#### **Claim 5**

Claim 5 recites: *[a]n information management apparatus according to claim 3, wherein the generating means generates the first authentication image containing a first amount of information based on a first amount of money...*

***“the first authentication image containing a first amount of information based on a first amount of money...”***

Claim 5 discloses that the authentication image includes “a first amount of information based on a first amount of money.”

Pare does not disclose that the first authentication image includes any monetary information. Even read in accordance with the arguments set forth in the final office action on page 4, reading the recited first authentication image on the biometric sample, Pare does not disclose that the biometric sample contains any monetary information. Instead, the biometric sample acts as a key to the user's financial records.

- Accordingly, Pare does not teach or suggest, nor would Pare motivate one of ordinary skill to produce a "*first authentication image containing a first amount of information based on a first amount of money...*" For similar reason claim 11 and 17 are also not taught or suggested by Pare.

Accordingly, Pare fails to disclose, teach, suggest or render obvious each and every feature of independent claims 3, 9-11, and 17, and dependent claims 4 and 5. Furthermore, claims 6, 8, 12, and 14 are also patentable over Pare because they depend on claims 3 or 11. Therefore, The rejection of claims 1-18 under 35 U.S.C. § 103(a) should be withdrawn.

### **CONCLUSION**

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 18-0013, under Order No. SON-2830 from which the undersigned is authorized to draw.

Dated: October 25, 2007

Respectfully submitted,

By

Ronald P. Kapanen

Registration No.: 24,104

Christopher M. Tobin

Registration No.: 40,290

RADER, FISHMAN & GRAUER PLLC

Correspondence Customer Number: 23353

Attorney for Applicant